THE HONORABLE JOHN C. COUGHENOUR

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA , Plaintiff, v. ROBERT J. HOWELL, Defendant.	CASE NO. CR21-0190-JCC ORDER

This matter comes before the Court on Defendant's motions to dismiss charges, compel discovery, suppress evidence, and/or for a *Franks* hearing (Dkt. Nos. 74, 107).[1] Having thoroughly considered the briefing and the relevant record, the Court DENIES Defendant's motions for the reasons explained herein.

I. BACKGROUND

After an investigation stemming from a 2019 tip, Defendant is charged with receipt and possession of child pornography. (Dkt. No. 94 at 1–2.) The tip came from a foreign law-enforcement agency (an "FLA") and stated that a specific internet provider ("IP") address was

[1] Defendant obtained new counsel between the submission of his original motion and his supplemental motion, (*See* Dkt. No. 98), and the latter preserves and focuses his submissions. (*See* Dkt. No. 107 at 3, 22–23.) The Court therefore focuses on the supplemental motion and briefing.

used to access five digital image and video files containing child sexual abuse material.[2] (Dkt. No. 75 at 3–4.)[3] The FLA also stated that the five files were accessed through a hidden website, which usually required users to create an account.[4] (*Id.*) Homeland Security Special Agent ("SA") Matthew Kimmel subpoenaed an internet service provider to identify the physical address corresponding to the IP address. (Dkt. No. 75-2 at 27.) According to that provider, Defendant was the owner and a resident of the property at that address. (*Id.*)

As part of his ensuing investigation, SA Kimmel reviewed a 2011police report regarding Defendant on child molestation allegations. (*Id.* at 28.) SA Kimmel also learned Defendant was the subject of 2012 and 2013 "Cybertips" from the National Center for Missing and Exploited Children ("NCMEC").[5] (*Id.* at 29–30.) The 2013 Cybertip contained information about four files uploaded to Google's Picasa application and flagged as suspected child pornography.[6] (*Id.* at 30.) The Cybertip included the e-mail address for the user that uploaded the files and a 2013

---

[2] The FLA tip indicated that the five files were named "2010 5yo kait little pussy.avi," "2010 Kait – toiletpee.avi," "2010 Kait 5YO anal dildo .wmv," "felixxx161314oub6yoanalrapedbytwoasstr," and "Vagina-Asshole.wmv." (Dkt No. 75 at 4.)

[3] Included in the record before the Court are the FLA tip, (Dkt. No. 75), the first warrant and supporting affidavit to search four image files, (Dkt. No. 75-1), and the second warrant and supporting affidavit to search Defendant's residence and person, (Dkt. No. 75-2).

[4] Internet websites and users may be hidden using The Onion Router ("Tor"), a service that obfuscates IP addresses through a series of relayed computers. (Dkt. No. 75-2 at 18–19.) A user's IP address is anonymized to computers further along the relay, making it even less visible to others (including law enforcement). (*Id.* at 19–20.) But, as Tor itself makes clear, a user's IP address is not completely anonymous—it can at least be identified by the first computer in the relay. (*See* Dkt. No. 84 at 5.)

[5] Certain electronic communication service providers, including Google, have statutory obligations to report to NCMEC any files that they suspect to be child pornography. *See* 18 U.S.C. § 2258A(a). NCMEC, in turn, has an obligation to relay this information to law enforcement, as was done here. *Id.* § 2258A(c).

[6] Service providers like Google do not have employees view every file they flag as child pornography. *See United States v. Wilson*, 13 F.4th 961, 964–65 (9th Cir. 2021). Instead, they have automated some of the process by attaching hash values to image files that are known to be child pornography. *See id.* When these hash values appear with image files on their servers, a Cybertip can be generated without an employee viewing the file. *See id.* at 972.

subpoena revealed that e-mail address belonged to Defendant. (*Id.* at 30–31.) Google could not verify whether one of its employees had viewed the files before alerting NCMEC. (Dkt. No. 75-1 at 13.) Without a warrant, SA Kimmel viewed the four files. (*See id.* at 13.) Then, out of "an abundance of caution," he obtained the first warrant to view the files. (*Id.* at 13, 17.) He did not relay to the magistrate what he saw and disclaimed any reliance on what he saw to establish probable cause. (*Id.* at 13.) The images he reviewed depicted child pornography. (*See* Dkt. No. 75-2 at 30–31.)

SA Kimmel applied for a second warrant one month later to search Defendant's residence and person for child pornography. (Dkt. No. 75-2 at 50.) His affidavit recapped the investigation to that point, including the FLA that provided Defendant's IP address, the prior molestation allegations, the NCMEC Cybertips, and a description of the four images he viewed. (*Id.* at 24–33.) SA Kimmel explained that these past events were material because individuals who possess child pornography often retain such material for "many years" (especially at their residences). (*Id.* at 38–39.) He also stated that the computer server hosting the hidden website "was seized by a foreign law enforcement agency" in 2019. (*Id.* at 21.) The second warrant issued, which law enforcement used to search Defendant's residence and seize child pornography found there. (Dkt. No. 1 at 3–4.)

Defendant now challenges both warrants on Fourth Amendment grounds and asks that the fruits of both be suppressed pursuant to the exclusionary rule. (*See generally* Dkt. Nos. 74, 107.) He argues that the first warrant was tainted by the prior warrantless search of the four image files. (Dkt. No. 107 at 4–10.) The Government admits the original search was illegal for the purposes of this motion but maintains that two exceptions to the exclusionary rule apply. (Dkt. No. 82 at 31–35.) Defendant argues that the second warrant is invalid because SA Kimmel misled the magistrate by failing to clearly disclose that there was not one but two relevant FLAs: one that seized the website and one that provided the IP address. (Dkt. No. 107 at 11–19.) This deception, Defendant submits, justifies a hearing under *Franks v. Delaware*, 488 U.S. 154

(1978), on the veracity of the affidavit. (Dkt. No. 107 at 18.) The Government responds that, while it is possible that the two FLAs could be a confusing detail, this does not rise to the level of materiality sufficient to justify questioning a facially valid warrant. (Dkt. No. 108 at 1–4.)

II. DISCUSSION

The Fourth Amendment prohibits unreasonable government searches and requires probable cause to justify a search warrant. U.S. Const. amend. XIV. The fruits of a prohibited search are considered tainted and may be suppressed pursuant to the exclusionary rule. *Mapp v. Ohio*, 367 U.S. 643, 648–49 (1961). The Government here is right to concede that the warrantless search of the four image files was prohibited. (Dkt. No. 82 at 33 n.6) (citing *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). The Ninth Circuit has held (in a decision after the warrant issued in this case) that viewing image files referenced in a Cybertip is not covered by the private search exception to the Fourth Amendment, and is therefore prohibited, when there is no evidence that the service provider's employees viewed the files (as here). *Wilson*, 13 F.4th 961 at 980. Therefore, some other exception is required, otherwise the fruits of the first warrant—the descriptions of the four images depicting child pornography—must be suppressed, including in the probable cause affidavit for the second warrant.

If a search is illegal, as admitted here, then it is the Government's burden to support an exception to the exclusionary rule. *Brown v. Illinois*, 422 U.S. 590, 604 (1975). The Fourth Amendment and the exclusionary rule are strict tenets that come with a tension: the Amendment's bounds are jealously guarded, but the costs of suppressing valid evidence are high. *See Davis v. United States*, 564 U.S. 229, 237–38 (2011) (explaining the "cost-benefit analysis"). There are thus numerous judge-made exceptions to the judge-made exclusionary rule. *See Utah v. Strieff*, 579 U.S. 232, 238 (2016) (listing some exceptions). These exceptions are instructed by the purpose of the rule: to deter Fourth Amendment violations. *See Davis*, 564 U.S. at 237. The two exceptions the Government offers here are good faith on SA Kimmel's part and attenuation between the prohibited search and the valid search. (Dkt. No. 82 at 31–34.) As with other

exceptions, good faith and attenuation both recognize that if the high costs of the exclusionary rule are not justified by deterrence, then the rule should not apply.

A. Good Faith Exception to a Warrantless Search

In *United States v. Leon*, the Supreme Court recognized that it is pointless to sanction a law enforcement officer with the exclusionary rule in the absence of their culpability. 468 U.S. 897, 918 (1984). In other words, suppression has no deterrent effect when the officer believes, in good faith, that the search was lawful. Courts have recognized that officers may rely in good faith on a valid search warrant, *id.* at 925, a state statute, *Illinois v. Krull*, 480 U.S. 340, 360 (1987), or binding appellate precedent, *Davis*, 564 U.S. at 241, even when those sources of law are later invalidated. An officer must rely on some source of law to implicate the good faith exception.

But here, the Government does not offer any source of law on which SA Kimmel could have relied to open the files associated with the 2013 Cybertip. (*See generally* Dkt. No. 82.) It cannot be a warrant because Kimmel viewed the images *before* he obtained the valid warrant. The Government does not point to a statute, either. And all it can say about legal precedent is that the law around Cybertips was "unsettled" at the time of the warrantless search, (Dkt. No. 82 at 32), which is insufficient. *See Davis*, 564 U.S. at 239 (addressing good faith reliance on "binding judicial precedent"); *United States v. Lara*, 815 F.3d 605, 613 (9th Cir. 2016) ("declin[ing] to expand the [good faith] rule in *Davis* to cases in which the appellate precedent, rather than being binding, is (at best) unclear").

The Ninth Circuit recently clarified that the good faith exception requires a binding appellate decision that "specifically authorizes" the conduct in question. *United States v. Holmes*, 121 F.4th 727, 737 (9th Cir. 2024). The Government offers *United States v. Lustig*, 830 F.3d 1075, 1082 (9th Cir. 2016), for the proposition that SA Kimmel does not need a perfectly analogous case to establish his good faith. (Dkt. No. 82 at 32.) But there, the government still offered *a case* on which the officer could have relied. *See Lustig*, 830 F.3d at 1084 (officer relied

in good faith on *United States v. Robinson*, 414 U.S. 218 (1973)). Here, the Government does not point to any case, or any other source of law, that specifically authorized the warrantless search under the good faith exception. Therefore, this exception does not apply.

B. Attenuation Exception to a Warrantless Search

While the good faith exception accounts for confusing or competing legal constraints on law enforcement, the attenuation exception recognizes that the connection between the fruit and the poisonous tree may be "so attenuated as to dissipate the taint." *Segura v. United States*, 468 U.S. 796, 805 (1984). This exception requires a fact-intensive inquiry. *United States v. Garcia*, 974 F.3d 1071, 1076 (9th Cir. 2020).

Again, the fruit in this case is the description of the four images from the 2013 Cybertip—SA Kimmel obtained this evidence by viewing the images both before and after the search warrant issued. The poisonous tree is SA Kimmel's first, warrantless viewing of those images. The question, then, is whether the descriptions were obtained sufficiently independent of the first viewing. If not, then the information Kimmel gained should "not be used at all." *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920) (invalidating subpoena based on information obtained in illegal seizure).

In *Utah v. Strieff*, the Supreme Court observed that an attenuated connection between the officer's misconduct (there, an illegal arrest without probable cause) and the discovery of evidence (drugs on the defendant's person) removes some of the exclusionary rule's sting. 579 U.S. at 241–42. Three factors are relevant to attenuation, according to *Strieff*. *Id.* at 239. First, the time between the misconduct and the discovery of evidence is a relevant factor. *Id.* There is no dispute here that the time between the warrantless viewing and the valid search warrant was so minimal as to weigh in favor of exclusion. (*See* Dkt. Nos. 82 at 33, 107 at 8.) But the other two factors are at issue: the intervening circumstance of the valid search warrant and the flagrancy of SA Kimmel's misconduct.

1. Intervening Circumstance

Circumstances that are sufficiently independent to sever the fruit from the poisonous tree include a prior-issued arrest warrant, as in *Strieff*. 579 U.S. at 240. That warrant was "wholly independent" of the illegal arrest and "broke" the connection with the drug evidence. *Id.* at 242. An independent circumstance may also be a later-issued search warrant, when the misconduct is an illegal search as in *Segura*. 468 U.S. at 814. There, probable cause for the later-issued warrant was obtained and presented to a magistrate prior to the illegal entry of the defendant's apartment. *Id.* at 801. Officers obtained evidence of drug trafficking as a result of the warranted entry. *Id.* The Court held that the evidence need not be suppressed because the illegal search was not even a "but for" cause that the evidence was discovered. *Id.* at 816;[7] *see also James v. United States*, 418 F.2d 1150, 1152 (D.C. Cir. 1969) ("If the lawfully obtained information amounts to probable cause and would have justified issuance of the warrant, apart from the tainted information, the evidence seized pursuant to the warrant is admitted.") Evidence will not be suppressed even if a warrant is sought subsequent to the misconduct, so long as the probable cause is disconnected from the illegal search and the officer would have sought the warrant prior to the search. *Murray v. United States*, 487 U.S. 533, 542 (1988). The exclusionary rule is meant to discourage a "search first, warrant later mentality." *Id.* at 540 n.2. Otherwise, officers could engage in suspicionless searches, find evidence of wrongdoing, and then seek a warrant, circumventing the Fourth Amendment altogether. But the exclusionary rule is meant to return the status quo as if the search had not occurred; it is not meant to put the Government in a worse position. *Id.* at 542.

An analogous fruit and tree to those here is found in *U.S. v. Mulder*. 889 F.2d 239 (9th Cir. 1989). There, officers had valid possession of some pills (which turned out to be drugs) because defendant left them in a hotel room and a hotel employee found them. *U.S. v. Mulder*,

[7] *Segura* was decided based on the related "independent source" exception, although it also cites *Silverthorne* and discusses attenuation. 468 U.S. at 814–15. Both the attenuation and independent source exceptions address "the causal relationship between the unconstitutional act and the discovery of evidence," and are thus relevant. *Strieff*, 579 U.S. at 238.

808 F.2d 1346, 1347–48 (9th Cir. 1987). Similarly here, there is no suggestion that Google wrongfully turned over Defendant's files to NCMEC who, in turn, passed them on to the Government. The question is about the search, not the seizure.

In *Mulder*, the officers could observe distinctive markings on the pills that were indicative of illegal drugs. 889 F.2d at 241. They had the pills tested without first obtaining a warrant—this constituted an illegal search. *Mulder*, 808 F.2d at 1348–49. But they later sought a search warrant to test the drugs. *Mulder*, 889 F.2d at 241. They presented a magistrate with a full and truthful affidavit, including the details about the prior testing, but disclaimed any reliance on that testing to establish probable cause. *Id.* at 242. The magistrate then granted a warrant, and the officers conducted a second round of testing that confirmed the pills were drugs. *Id.* at 240. The Ninth Circuit declined to suppress the results of the second test because sufficient probable cause (the markings on the pills) existed before the illegal search. *Id.* at 241 (citing *Murray*, 487 U.S. at 542 n.3).

Similarly here, SA Kimmel had suspicion and probable cause *before* he opened the files and presented that information to the magistrate. (*See generally* Dkt. No. 75-1 at 5–14.) His investigation was initiated based on the 2019 FLA tip that tied Defendant to child sexual abuse material. SA Kimmel presented to the magistrate the 2011 child molestation investigation, the 2012 Cybertip, as well as the 2013 Cybertip that contained the four relevant files. The 2013 Cybertip also contained an e-mail address attributed to Defendant by the 2013 Google subpoena. The magistrate could rely on all of this information—obtained prior to and independent of the illegal search—to find probable cause, as in *Mulder*. Then, the magistrate issued a warrant that commanded execution by a date certain. (*Compare* Dkt. No. 75-1 at 17 ("YOU ARE COMMANDED to execute this warrant . . ."), *with Garcia*, 974 F. 3d at 1077 (defendant's probation condition only provided discretion for search, while a warrant is a "judicial mandate that an officer has a sworn duty to carry out").

The warrant would not have been independently sufficient, however, if it were a purely post-hoc justification for an illegal search. The Ninth Circuit held as much in *United States v. Taheri* because the probable cause was developed *after* the illegal search, not before. 648 F.2d 598, 600 (9th Cir. 1981). All the government could rely on that predated the misconduct there was an "informant of unknown reliability." *Id.* at 599. Whereas SA Kimmel relied on credible and pre-existing information to establish probable cause independent of what he saw in the four images. He did not go fishing in Defendant's files without suspicion, nor is there evidence that his decision was "significantly directed" by what he first viewed. *Cf. United States v. Gorman*, 859 F.3d 706, 716 (9th Cir. 2017) (decision to conduct a dog sniff was a direct result of suspicion gained from unlawful detention). In this instance, a judicial officer issued a warrant that instructed a search. This is therefore a sufficient circumstance that weighs in favor of an exception to the exclusionary rule.

2. Flagrancy of Misconduct

The final factor discussed in *Strieff* is the flagrancy of the officer's misconduct. 579 U.S. at 241. The Court stated this factor is "particularly significant." *Id.* at 239. The flagrant misconduct must rise to a level above the absence of proper cause. *Id.* at 243. It may be, for example, a suspicionless fishing expedition in someone's home. *See id.* at 242; *see also Garcia*, 974 F.3d at 1080–81. Defendant here does not suggest that SA Kimmel's conduct is flagrant in the sense that it invaded his private residence or seized and rifled through his personal effects. (*See generally* Dkt. Nos. 74, 107.) Indeed, it would be difficult to call viewing four specific image files flagged as child pornography by Google and NCMEC a fishing expedition. Nor does Defendant suggest that Kimmel was untruthful with the magistrate in his affidavit; if anything, his suggestion is that Kimmel was *too* truthful. Defendant argues that SA Kimmel's affidavit was flagrant misconduct because it was a "wink, wink, nudge, nudge" submission to the magistrate about the already-viewed files, which necessarily tainted the warrant. (Dkt. No. 107 at 10.)

Mulder also addresses this argument. It found that telling a magistrate about a prior illegal search—there, going further and revealing that the pills tested positive as drugs—is not dispositive on the validity of the warrant. *Mulder*, 889 F.2d at 242. In there as here, the officer disclaimed any reliance on the illegal search for probable cause and then a neutral magistrate issued a warrant. (*Compare id.*, *with* Dkt. No. 75-1 at 13.) The Ninth Circuit noted that the affiant had to disclose the prior search in the interest of truthfulness. *Mulder*, 889 F.2d at 242 n.2.

Officers should not be caught between a *Franks* hearing for untruthfulness, *see infra* Part II(C), and a rule that punishes too much truth. Instead, the neutral magistrate serves an independent and important check. They are capable of evaluating probable cause on the submissions of the government, including when asked to rely on certain information and not other information. *Cf. Illinois v. Gates*, 462 U.S. 213, 236 (1983) ("A magistrate's determination of probable cause should be paid great deference by reviewing courts.") SA Kimmel did not inevitably taint the warrant by telling the magistrate the truth. The magistrate could still have refused the warrant but, as discussed above, they found sufficient probable cause in the pre-existing information. This Court does not find otherwise.

In summary, SA Kimmel viewed four digital images that came in with a Cybertip. Soon thereafter, he realized he should have a warrant and obtained one. This permitted him to view and describe the four images in the affidavit for a second warrant. "[T]hese errors in judgment hardly rise to a purposeful or flagrant violation of [Howell's] Fourth Amendment rights." *Strieff*, 579 U.S. at 241. Therefore, the officer's misconduct was not flagrant.

Of the three relevant factors, two weigh against suppression under the attenuation exception to the exclusionary rule. Therefore, the Court finds that suppression of the image descriptions discovered from the first warrant is not justified.

C. *Franks* Hearing

Defendant challenges the second warrant (for the search of his residence and person) on the ground that SA Kimmel's affidavit misled the magistrate. (Dkt. No. 107 at 11–19.) Thus,

Defendant submits, the warrant was not supported by probable cause and the search was a Fourth Amendment violation. (*Id.* at 19–20.) Defendant's supplemental motion focuses on the fact that there were two FLAs, not just one. (*Id.* at 16–18.) Defendant suggests that this matters for two reasons. First, it matters because the magistrate may have thought that there was only one FLA. (*Id.* at 17.) Second, it matters because an FLA may have actually seized Defendant's computer[8] when the FLA stated it did not, and SA Kimmel repeated the same to the magistrate. (*Id.* at 17–18) (*see also* Dkt. No. 75-2 at 25). If Defendant can meet the standard for material falsity laid out in *Franks v. Delaware*, then he is entitled to a hearing on the veracity of the search warrant affidavit. 438 U.S. at 154.

The rule announced in *Franks* is one of "very limited scope." *United States v. Chesher*, 678 F.2d 1353, 1360 (9th Cir. 1982). There is "a presumption of validity with respect to the affidavit supporting the search warrant." *Franks*, 438 U.S. at 171. In order to overcome this presumption, a defendant must make a "substantial preliminary showing" that is more than "conclusory." *Id.* at 155, 171. A defendant must show that the affidavit contains (1) an intentional or reckless (2) falsity that is (3) material to probable cause. *Id.* at 155–56. "Allegations of negligence or innocent mistake are insufficient." *Id.* at 171. The false statement may be affirmative. *Id.* at 158. Or it could be false by reckless omission. *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985) (affidavit stating a material event occurred at the defendant's residence, but the affiant knew the defendant did not reside there at the time of the event). Falsity by commission or omission must be material to the magistrate's probable cause finding to trigger a hearing. *Franks*, 438 U.S. at 171.

Here, Defendant's arguments fail on all three elements, therefore there has not been a substantial showing to justify a hearing.

---

[8] In this context, Defendant claims that a "seizure" of his computer would have been accomplished by infecting it with software that recorded and transmitted his IP address. (Dkt. No. 74 at 13.) Defendant suggests in his initial motion this is the only way his IP address could have been obtained, (*id.*), which the Government disputes, (Dkt. No. 82 at 10–11).

First, the Court finds it unlikely that the few words that describe the seizing FLA were intentionally misleading. In the forty-page affidavit, the sole mention of this FLA is the following: "In June of 2018, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency." (Dkt. No. 75-2 at 21.) SA Kimmel did not refer to this entity with the abbreviation "FLA." (*Id.*) He provided this information as background, several pages before turning to the probable cause for the proposed search. (*See* Dkt. No. 75-2 at 24). It is there in the affidavit that SA Kimmel precisely defines "FLA": "In August 2019, a foreign law enforcement agency (*referred herein as 'FLA'*) . . . notified the FBI that FLA determined that on April 21, 2019, [Defendant's] IP address . . . 'was used to access online child sexual abuse and exploitation material.'" (Dkt. No. 75-2 at 24–25) (emphasis added) (citation to source material omitted). Indeed, all subsequent references to "FLA" refer solely to the tipping FLA. (*See generally* Dkt. No. 75-2 at 24–50.) This seems to the Court to be an intentional distinction, if anything. Nor does it seem to the Court that SA Kimmel was reckless, given the care he displayed in defining and consistently using "FLA" in establishing probable cause before the magistrate. At best, SA Kimmel made a mistake by omission, which is insufficient under *Franks*.

Second, the Court does not find that the affidavit contains false information about the FLAs, either. The Government concedes that an extra sentence about the two FLAs would have made the affidavit clearer. (Dkt. No. 108 at 4.) But a lack of clarity is not a falsity (even with the help of "linguistic gymnastics"). (*See* Dkt. No. 109 at 4.) And it is Defendant's burden to make a substantial showing that the references to the FLAs are somehow false. *See Franks*, 438 U.S. at 171. Confusing they could be, but false they are not. The magistrate, if they had been confused, could have so indicated before issuing the warrant. But they did not.

As for what an FLA did to obtain Defendant's IP address, the affidavit only repeated what the FLA said: "FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to

obtain that IP address information." (Dkt. No. 75-2 at 25; *see also* Dkt. No. 75 at 2 (FLA stating the same).) Defendant does not point to any authority for the proposition that the affidavit must establish *how* the IP address was obtained by a foreign entity.[9] All he offers is the following conclusory assertion: "There are presently no publicly known methods of de-anonymizing the IP address of a Tor user that does not require interference with the subject computer." (Dkt. No. 107 at 13; s*ee also* Dkt. No. 74 at 2 (alleging infection with malware).) This is just conjecture about "outrageous conduct," *United States v. Anzalone*, 923 F.3d 1, 5 (1st Cir. 2019), not submissions toward a substantial showing. *See Franks*, 438 U.S. at 171 ("Affidavits or sworn or otherwise reliable statements of witnesses should be furnished").

Third, and most importantly, even if the two FLAs and their roles were clarified, that would not change the relevant inferences the magistrate could make to establish probable cause. Here, a law-abiding and reliable FLA provided a tip that an IP address in the United States was used to access child pornography. SA Kimmel used that IP address to obtain an associated physical address—Defendant's residence. SA Kimmel also conducted an investigation into Defendant that turned up prior reports, Cybertips, and eventually four images depicting child

---

[9] This is one of several pieces of information that Defendant observes are not in the affidavit. (*See, e.g.,* Dkt. No. 74 at 5, 7.) While it is not the Government's burden, it has, in the course of briefing the instant motion, offered an expert's declaration as to the technical possibility of obtaining an IP address without seizure and explains that at least one of the computers along the Tor relay obtains a user's IP address. (Dkt. No. 84 at 4–5.)

Defendant said in his initial motion that he has an expert on Tor servers, (Dkt. No. 74 at 17), but that was before Defendant understood there were two FLAs and, regardless, no such witness submission is now before the Court. Furthermore, there is no evidence this case is like the "Playpen" cases Defendant alludes to in his initial motion. *United States v. Henderson*, 906 F.3d 1109 (9th Cir. 2018); *United States v. Vortman*, 801 Fed. Appx. 470 (9th Cir. 2020). Defendant's IP address was provided by an FLA, not a United States Government investigation. Defendant wisely stays away from this position in his supplemental and supplemental reply briefing. (*See generally* Dkt. Nos. 107, 109.)

The Government also maintains that it has not cut off discovery, and "will continue to provide discovery," (Dkt. No. 82 at 37), so the Court leaves it to the parties to continue that process. If necessary, Defendant may renew his motion to compel discovery, including with respect to information about the FLAs. (*See* Dkt. No. 107 at 23.)

pornography uploaded to an internet account in Defendant's name. And as SA Kimmel explained, child pornography is often kept for years at the offenders' residence. Even if the affidavit "insert[ed] the omitted truth," *United States v. Ippolito*, 774 F.2d 1482, 1486 n.1 (9th Cir. 1985), it would not change the finding of probable cause to search Defendant's residence and person for child pornography based on all the other information in the affidavit. Even if intentional or false, what Defendant alleges is not material to the magistrate's finding. Therefore, it is not enough to justify a *Franks* hearing, and the conduct is certainly insufficient to dismiss the indictment.

III. CONCLUSION

While SA Kimmel no doubt conducted a warrantless search, the subsequent and independently supported warrant justifies an exception to the exclusionary rule. Nor does his conduct rise to the level of flagrancy requiring exclusion. In addition, to the extent that his affidavit was confusing, any resulting confusion was immaterial. This does not justify a *Franks* hearing. Therefore, the Court FINDS both warrants valid, as were the fruits of the resulting searches.

For the foregoing reasons, Defendant's motions (Dkt. No. 74, 107) are DENIED.

DATED this 21st day of January 2025.

John C. Coughenour
UNITED STATES DISTRICT JUDGE